Kaseya 2

AntiMalware

Guía del usuario

Versión 7.0

Español

January 6, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2014 Kaseya. All rights reserved. | www.kaseya.com

Contenido

Introducción a AntiMalware **1**
Requisitos del módulo AntiMalware **3**
Máquinas **3**
- **Diseño de página** **3**
- **Cuadrícula de explorador** **4**
- **Panel de control** **5**
- **Columnas de AntiMalware** **8**
- **Panel de detalles** **9**

Tableros **11**
Detecciones **11**
Perfiles **12**
- **Pestaña Resumen** **13**
- **Pestaña Protección** **13**
- **Pestaña Análisis AM** **14**
- **Pestaña Opciones de actualización** **15**
- **Pestaña Exclusiones** **15**
- **Pestaña Extremos** **16**

Alertas **16**
- **Pestaña Resumen** **17**
- **Pestaña Tipos de alerta** **17**
- **Pestaña Acciones** **18**
- **Pestaña Extremos** **18**

Índice **19**

Introducción a AntiMalware

AntiMalware (KAM) proporciona seguridad de extremo de Anti-Malware Pro de Malwarebytes para las máquinas administradas. **AntiMalware** se puede instalar en forma independiente de **Endpoint Security** o **Antivirus**. **AntiMalware** es particularmente eficaz en la detección y prevención de spyware de *software de seguridad falso (scareware)* o *antivirus falso* que instala un virus y después intenta cobrarle al cliente para eliminarlo.

AntiMalware detecta, destruye y bloquea rápidamente el software malintencionado. Se controlan todos los procesos y se detienen los malintencionados antes de que comiencen. Tanto el análisis como la protección en tiempo real utilizan tecnología de detección heurística avanzada para mantener los sistemas a salvo, incluso contra las amenazas de malware más recientes.

- Compatible con Windows 2000, XP, Vista, 7, 8 y 8.1 (de 32 bits y 64 bits).
- Análisis de alta velocidad.
- Capacidad de realizar análisis completos de todas las unidades.
- Publicación diaria de actualizaciones de bases de datos que protegen contra el malware más reciente en estado salvaje.
- La heurística inteligente detecta hasta el malware más persistente sin aplicar una carga excesiva sobre los recursos de sistema.
- Protección en tiempo real que controla el sistema de archivos y el tráfico de Internet.
- Programador para mantener la protección actualizada automáticamente.
- Cuarentena para contener las amenazas y realizar restauraciones según sea conveniente.
- Lista de omitidos lista tanto para el detector como para el módulo de protección.
- Puesta en cuarentena automática de amenazas.
- Sin necesidad de reinicio después de la instalación.
- La protección controla toda la máquina, más allá de las cuentas individuales.
- Compatible con exclusiones de archivos, carpetas, claves y valores de registro y direcciones IP4.
- La administración de directivas puede administrar la asignación de perfiles de AntiMalware.

Caché de LAN

La memoria caché de LAN permite que varias máquinas recuperen los mismos archivos desde una máquina LAN local en lugar de descargarlos de manera reiterada deKaseya Server. Esto reduce los problemas de ancho de banda de la red. Los archivos que se descargan para los extremos de **AntiMalware**, excepto las actualizaciones del archivo de firmas de Malwarebytes, usan la memoria caché de LAN automáticamente si ya está configurada para dichos extremos. No se necesita configuración adicional en **AntiMalware**. Para obtener más información, consulte **Memoria caché de LAN** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#9328.htm)* en Agente.

> Nota: Consulte **Requisitos del sistema de AntiMalware** *(página 3)*.

Funciones	Descripción
Máquinas *(página 3)*	Permite instalar el software AntiMalware en las máquinas seleccionadas y desinstalarlo de ellas, y proporciona una vista detallada del estado de AntiMalware de cualquier máquina seleccionada.
Tableros *(página 11)*	Muestra una vista de tablero del estado de todas las máquinas que tienen instalado AntiMalware.
Detecciones *(página 11)*	Muestra las amenazas de virus sobre las que puede actuar.
Perfiles *(página 12)*	Permite administrar los perfiles de AntiMalware que se

	asignan a los ID de máquina.
Alertas *(página 16)*	Permite administrar las alertas de los módulos AntiMalware.

Requisitos del módulo AntiMalware

Kaseya Server

- El módulo AntiMalware 7.0 requiere el VSA 7.0.

Requisitos para todas las estaciones de trabajo administradas

- Procesador de 500 MHZ
- 256 MB de RAM
- 15 MB de espacio libre en disco
- Microsoft Windows XP SP2, Vista, 7, 8, 8.1. Los sistemas Apple y Linux no son compatibles.
- Consulte **Requisitos del sistema** *(https://www.malwarebytes.org/business/antimalware/)* en Malwarebytes para obtener más información.

Nota: Consulte **Requisitos generales del sistema** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/reqs/index.asp#home.htm)*.

Máquinas

AntiMalware > Mostrar > Administrar máquinas

En la página **Máquinas**, se puede instalar y desinstalar el software **AntiMalware** en las máquinas seleccionadas. En esta misma página se proporciona una vista detallada del estado de **AntiMalware** de cualquier máquina seleccionada.

- **Diseño de página** *(página 3)*
- **Cuadrícula de explorador** *(página 4)*
- **Panel de control** *(página 5)*
- **AntiMalware Columnas** *(página 8)*
- **Panel de detalles** *(página 9)*

Diseño de página

La composición de la página **Máquinas** *(página 3)* comprende los siguientes elementos de diseño:

- **Panel de navegación**: se usa para navegar a las páginas dentro del módulo **AntiMalware**.
- **Cuadrícula de explorador**: todas las máquinas administradas en el VSA se incluyen en este panel.
  - **Explorador de páginas**: si se muestra más de una página de dispositivos, se pueden avanzar o retroceder páginas.
  - **Filas por página**: establece la cantidad de dispositivos que se muestran por página (10, 30 o 100).
- **Filtro ID de máquina/ID de grupo**: filtra la lista de los ID de máquina que se incluyen en la **Cuadrícula de explorador**.
- **Panel de control**: ejecuta tareas, ya sea para toda la **Cuadrícula de explorador** o para una única máquina seleccionada.
- **Panel de detalles**: en este panel, se muestran las propiedades y el estado de una única máquina.
  - **Encabezado**: identifica la máquina seleccionada en la **Cuadrícula de explorador**.

- **AntiMalware**: muestra un resumen del estado de **AntiMalware** de una máquina.
- **Perfiles de alerta**: se enumeran los perfiles de alerta asignados a una máquina.

Cuadrícula de explorador

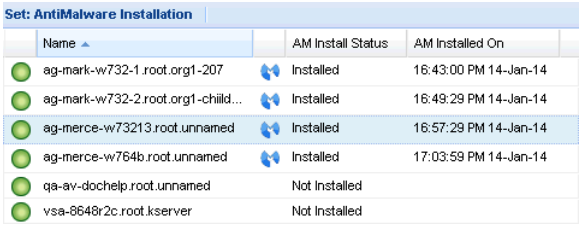
En la **Cuadrícula de explorador** de la página Máquinas, se enumeran todas las máquinas que actualmente tienen instalado **AntiMalware** *y* que se incluyen en el **filtro ID de máquina/ID de grupo** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)*.

Nota: La única excepción se da cuando está seleccionada la opción `Installation de AntiMalware`. En este caso, se muestran todas las máquinas que se incluyen en el filtro ID de máquina/ID de grupo.

- El *conjunto de columnas* que se muestra está determinado por la selección del **Conjunto de columnas** en el **Panel de control** *(página 5)*. El conjunto de columnas seleccionado actualmente se muestra en la barra que se encuentra encima de la **Cuadrícula de explorador**.

  Nota: Consulte **Columnas de AntiMalware** *(página 8)* para obtener una descripción de todas las columnas disponibles para mostrarse en *cualquier* conjunto de columnas de la **Cuadrícula de explorador**.

- La opción de avanzar página permite visualizar varias páginas de máquinas.
- La opción de máquinas por página permite establecer la cantidad de filas en cada página.



Íconos de columna

	Definiciones desactualizadas
	Reinicio requerido
	Análisis completo en curso
	Licencia caducada
	La configuración de extremo no cumple los requisitos del perfil
	Asignación pendiente
	Habilitación pendiente
	Deshabilitación pendiente
	Análisis pendiente
	Desinstalación pendiente
	Verificación Pendiente
	Instalación Pendiente

	Actualización pendiente
	Falló la Instalación
	Instalación correcta

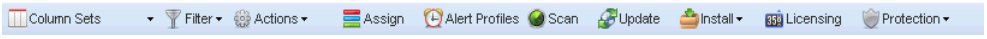
Convenciones de íconos de componentes

Si se mantiene el mouse sobre un ícono de componente, se muestra información sobre herramientas que describe el estado del componente. En general, se usan las siguientes convenciones de íconos de componentes.

Estado	Tipo de ícono mostrado	Ejemplo: Íconos de protección de archivo
Deshabilitado	X gris	
Falla	signo de exclamación amarillo	
En ejecución/habilitado	marca de verificación verde	
Iniciando	llave con flecha verde	
Detenido	X roja	
Deteniendo	llave con signo menos rojo	

Panel de control

El **Panel de control** que se encuentra en la parte superior de la página **Máquinas** *(página 3)* ejecuta tareas para toda la **Cuadrícula de explorador** *(página 4)* o para una única máquina seleccionada.



Conjuntos de columnas

Cuando se selecciona un conjunto de columnas, se muestra un conjunto de columnas predefinido.

- **Modificar columnas**: personaliza el conjunto de columnas que se muestra en *cualquier* conjunto de columnas.

  Nota: *Consulte* **Columnas de AntiMalware** *(página 8)* para obtener una descripción de todas las columnas disponibles para mostrarse en *cualquier* conjunto de columnas de la **Cuadrícula de explorador**.

- **Instalación de AntiMalware**: muestra las columnas de instalación de **AntiMalware** en la **Cuadrícula de explorador** *para todas las máquinas con agente*.
- **Estado de AntiMalware**: muestra las columnas de estado en la **Cuadrícula de explorador** para todas las máquinas con agente *que tienen un cliente de* **AntiMalware** *instalado.*

Filtro

Filtra la lista de filas que se muestran por software instalado, actualización recomendada, reinicio requerido, definiciones desactualizadas, máquina que no cumple los requisitos del perfil, versión más reciente instalada o clientes no compatibles.

Nota: El filtro `Upgrade Recommended de AntiMalware` lo ayuda a identificar cuáles son las máquinas que cumplen con los requisitos para la actualización a la versión más reciente. Para actualizar, realice la instalación sobre una instalación existente de **AntiMalware**.

Acciones

- **Cancelar acción pendiente**: cancela las acciones pendientes en las máquinas seleccionadas.
- **Reiniciar**: reinicia las máquinas seleccionadas.

Asignar

Asigna un perfil de configuración de **AntiMalware** a las máquinas seleccionadas. Consulte **Perfiles** *(página 12)* para obtener más información.

Perfiles de alerta

Asigna o quita un perfil de alerta para las máquinas seleccionadas. En la pestaña **Perfiles de alerta** en el **Panel de detalles** *(página 9)*, se muestran todos los perfiles asignados a una máquina.

Explorar

Programa un análisis de **AntiMalware** en las máquinas seleccionadas.

- **Fecha de inicio**: la fecha de inicio del análisis.
- **Hora**: la hora de inicio del análisis.
- **Período de distribución**: reprograma varios análisis de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.

Existen tres tipos de análisis para **AntiMalware**:

- **Análisis completo**: en este análisis, se analizan todos los archivos en las unidades seleccionadas. En la mayoría de los casos, se recomienda un análisis rápido.
- **Análisis rápido**: en este análisis, se utiliza una tecnología de análisis de sistemas veloz para detectar software malintencionado.
- **Análisis de flash**: en este análisis, se analizan la memoria y los objetos de ejecución automática.

Actualizar

Programa una actualización en las máquinas seleccionadas con las definiciones de **AntiMalware** más recientes.

- **Fecha de inicio**: la fecha de inicio de la actualización.
- **Hora**: la hora de inicio de la actualización.
- **Período de distribución**: reprograma varias actualizaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.

Instalar

- **Instalar o actualizar AntiMalware**: instala o actualiza el cliente de **AntiMalware** en las máquinas seleccionadas.
  - **Selección de perfil**: se pueden seleccionar e instalar estaciones de trabajo al mismo tiempo A las estaciones de trabajo se les asigna el perfil de estación de trabajo seleccionado.
  - **Opciones avanzadas**: haga clic para visualizar las siguientes opciones.
    - ✓ **Fecha y hora de inicio**: la fecha y la hora de inicio de la instalación.
    - ✓ **Período de distribución**: reprograma varias instalaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.

  - **Bloqueo de problemas en la instalación**: se enumeran los problemas que pueden evitar que la instalación se realice correctamente en las máquinas seleccionadas.
- **Desinstalar AntiMalware**: desinstala el cliente de **AntiMalware** en las máquinas seleccionadas.
  - **Fecha de inicio**: la fecha de inicio de la desinstalación.
  - **Hora**: la hora de inicio de la desinstalación.
  - **Período de distribución**: reprograma varias desinstalaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
- **Reparar la instalación de AntiMalware**: vuelve a instalar los archivos faltantes en un cliente de **AntiMalware** instalado previamente para repararlo. El cliente de **AntiMalware** se debe haber instalado previamente con **AntiMalware** para el mismo VSA.
  - **Fecha de inicio**: la fecha de inicio de la reparación.
  - **Hora**: la hora de inicio de la reparación.
  - **Período de distribución**: reprograma varias reparaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
- **Conectar Kaseya AntiMalware**: restablece una conexión a una máquina anteriormente administrada por **AntiMalware** a la que se le quitó el agente de Kaseya y luego se le volvió a instalar. Esto incluye el restablecimiento de una conexión a las máquinas que eran administradas por un VSA diferente.
  - **Fecha de inicio**: la fecha de inicio de la reparación.
  - **Hora**: la hora de inicio de la reparación.
  - **Período de distribución**: reprograma varias verificaciones de manera uniforme a lo largo de un período de distribución en un plazo inferior a la cantidad de períodos especificados, para distribuir el tráfico de red y la carga del servidor.
  - **Selección de AntiMalware**: selecciona el perfil de estación de trabajo que se aplica.

Licencias

- **Recuentos de licencias**: indica la cantidad de licencias de **AntiMalware** para estaciones de trabajo. La cantidad de licencias de **AntiMalware** también se muestra en la página **Administrador de licencias** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#2924.htm)* en Administración > Administrar.
  - Total comprados hasta la fecha
  - Completamente disponible (comprada no asignada, aplicada, parcial o vencida)
  - Asignada (programada para instalación, pero la instalación aún no está completa)
  - Aplicada (licencia activa aplicada a una máquina)
  - Parcialmente disponible (asignada antes a una máquina, pero devuelta al grupo antes del vencimiento)
  - Parcialmente asignada (disponibilidad parcial que se programó para la instalación, pero la instalación aún no está completa)
  - Total (licencias compradas menos las vencidas)
  - Licencias expiradas
  - Con vencimiento en los próximos 30 días
  - Con vencimiento en los próximos 60 días
  - Con vencimiento en los próximos 90 días

Protección

- **Obtener estado**: vuelve al estado habilitado o deshabilitado de los componentes de **AntiMalware** en una máquina y, si es necesario, corrige la vista de los íconos de estado del componente en la

Cuadrícula de explorador. Además, devuelve la información de versión de la firma de instalación y de base de datos.

- **Habilitar AntiMalware temporalmente**: vuelve a habilitar la protección de **AntiMalware** en las máquinas seleccionadas.
- **Deshabilitar AntiMalware temporalmente**: deshabilita la protección de **AntiMalware** en las máquinas seleccionadas. Algunas instalaciones de software requieren que se deshabilite **AntiMalware** para completar la instalación.

Columnas de AntiMalware

Los conjuntos de columnas determinan las columnas que se muestran en la **Cuadrícula de explorador** *(página 4)*. Puede editar *cualquier* conjunto de columnas que se indique en la lista desplegable **Conjunto de columnas** en el **Panel de control** *(página 5)*.

1. Seleccione un conjunto de columnas en la lista desplegable **Conjunto de columnas**.
2. Seleccione **Modificar columnas** en la misma lista desplegable para visualizar la ventana **Editar conjunto de columnas**.

   Las columnas asignadas en la lista de la derecha son las que se muestran cuando guarda cambios en el conjunto de columnas.

Las siguientes columnas están disponibles para seleccionarse cuando se modifica *cualquier* conjunto de columnas en la **Cuadrícula de explorador** *(página 4)*. Seleccione **Conjunto de columnas** en el **Panel de control** *(página 5)* para modificar un conjunto de columnas.

AntiMalware

- **Componentes de AM**: identifica el estado de los componentes de **AntiMalware** instalados en esta máquina.
- **Versión de base de datos de AM**: la versión de la base de datos de definiciones de **AntiMalware** que usa la máquina en este momento.
- **Fecha de caducidad de AM**: la fecha de vencimiento programada para la seguridad de **AntiMalware**.
- **Estado de instalación de AM**: `Not Installed`, `Script Scheduled`, `Installed`
- **Fecha de instalación de AM**: la fecha en que se instaló **AntiMalware**.
- **Última actualización de AM**: la fecha en que se actualizó la base de datos de definiciones de **AntiMalware** por última vez.
- **Perfil de AM**: el perfil de **AntiMalware** asignado a esta máquina.
- **Versión del programa AM**: el número de versión de Malwarebytes del cliente de **AntiMalware** instalado en esta máquina.
- **Versión de servicio de AM**: la versión del cliente de **AntiMalware**.
- **Indicadores de AM**: entre los posibles indicadores se incluye `Definitions out of date`
- **Ícono de fase de instalación de AM**: si está seleccionada, **AntiMalware** está instalado en la máquina.
- **Acciones pendientes de AM**: íconos que representan las acciones de instalación, asignación, actualización y análisis.

Protección de extremo

- **Cadena de GUID del agente**: el GUID único del agente de Kaseya en formato de cadena.
- **ID**: el GUID único del agente de Kaseya en formato numérico.
- **Último reinicio**: la fecha y la hora en que se reinició la máquina por última vez.
- **Nombre de inicio de sesión**: el usuario de la sesión actual.
- **Nombre**: el machine ID.group ID.organization ID de la máquina.
- **Estado en línea**: Estos íconos indican el estado de registro del agente de cada máquina administrada. Al mantener el mouse sobre un ícono de registro, se muestra la ventana de QuickView del agente.

- En línea pero esperando que se completa la primer auditoría
- Agente en línea
- Agente en línea y usuario actualmente conectado.
- Agente en línea y usuario actualmente registrado, pero el usuario ha estado inactivo durante 10 minutos.
- Agente actualmente fuera de línea
- Agente no se ha registrado nunca
- Agente en línea pero el control remoto se ha deshabilitado
- El agente ha sido suspendido

- **Sistema operativo**: el sistema operativo de la máquina.
- **Ajuste de zona horaria**: muestra la cantidad de minutos. Consulte Sistema > Configuración del usuario > **Preferencias** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#503.htm)*.

Explorar

- **Último análisis de flash de AM**: la fecha y la hora en que se realizó el último análisis de flash de **AntiMalware**. En el análisis de flash, se analizan la memoria y los objetos de ejecución automática.
- **Último análisis completo de AM**: la fecha y la hora en que se realizó el último análisis completo de **AntiMalware**. En el análisis completo, se analizan todos los archivos en las unidades seleccionadas. En la mayoría de los casos, se recomienda un análisis rápido.
- **Último análisis rápido de AM**: la fecha y la hora en que se realizó el último análisis rápido de **AntiMalware**. En el análisis rápido, se utiliza una tecnología de análisis de sistemas veloz para detectar software malintencionado.

Estado

- **Acciones pendientes**: instalación, asignación, actualización y análisis.
- **Reinicio requerido**: si se lee `Yes`, se requiere un reinicio.

Actualización lista

- **Versión disponible del cliente de AM**: el número de versión de Malwarebytes del cliente de **AntiMalware** disponible para actualizar en esta máquina.

Centro de seguridad de Windows

- **Activo**: si está seleccionada, el producto antivirus está en uso.
- **Fabricante**: el fabricante del producto antivirus.
- **Actualizado**: si está seleccionada, el producto antivirus está actualizado.
- **Versión**: la versión del producto antivirus.
- **Nombre del producto informado al WSC**: el nombre del producto antivirus registrado con el *Centro de seguridad de Windows* (WSC). **AntiMalware** en sí no se registra con el *Centro de seguridad de Windows*.

> **Nota:** En Windows 7 y versiones posteriores, el *Centro de seguridad de Windows* se denomina *Centro de actividades*.

Panel de detalles

Encabezado

- **Nombre**: el machine ID.group ID.organization ID de la máquina.
- **SO**: el sistema operativo de la máquina.

- **Dirección IP**: la dirección IP de la máquina.
- **ID de agente**: el GUID del agente en la máquina administrada.

Pestaña de estado

- **Estado de instalación**: si está seleccionada, la seguridad de **AntiMalware** está instalada. Seleccione Ver registro para ver el registro de la máquina.
- **Fecha de instalación**: la fecha en que se instaló **AntiMalware**.
- **Error de instalación**: si se produce un error de instalación, se muestra un vínculo `View Log` al registro de instalación.
- **Vencimiento de licencia**: la fecha de vencimiento programada para la seguridad de **AntiMalware**.
- **Perfil**: el perfil de configuración de **AntiMalware** asignado a esta máquina.
- **Último análisis completo**: la fecha y la hora en que se realizó el último análisis de todos los archivos en las unidades seleccionadas con **AntiMalware**.
- **Último análisis rápido**: la fecha y la hora en que se realizó el último análisis rápido con **AntiMalware** para detectar software malintencionado.
- **Último análisis de flash**: la fecha y la hora en que se realizó el último análisis de flash con **AntiMalware** de la memoria y los objetos de ejecución automática.
- **Próximo análisis completo**: la fecha y la hora programadas para el próximo análisis de **AntiMalware**.
- **Versión de antimalware de Malwarebytes**: el número de versión de Malwarebytes del cliente de **AntiMalware** instalado en esta máquina.
- **Versión de administración**: la versión de Kaseya del servicio **AntiMalware** instalado.
- **Versión de la base de datos**: el número de versión de Malwarebytes de la base de datos de definiciones de **AntiMalware**.
- **Fecha de base de datos**: la fecha y la hora de la base de datos de definiciones de **AntiMalware** que usa la máquina en este momento.
- **Indicadores**: entre los posibles indicadores se incluyen `Definitions out of date`, `Out of Compliance`.

  > **Nota:** Una vez que la máquina vuelve a cumplir con los requisitos, el indicador de falta de cumplimiento de los requisitos se sigue mostrando. Para que el indicador de falta de cumplimiento de los requisitos deje de aparecer, vuelva a asignar el perfil a la máquina.

- **Estado del componente**: identifica el estado de los componentes de **AntiMalware** instalados en esta máquina.

  El servicio está en ejecución o detenido.

  El módulo de protección está en ejecución o detenido.

  El bloqueo de ejecución de archivo está en ejecución o detenido.

  El bloqueo de sitios web malintencionados está en ejecución o detenido.

Pestaña Perfiles de alerta

Se muestra la lista de perfiles de alerta asignados a la máquina seleccionada.

> **Nota:** En la pestaña Extremos, en Alertas > <perfil>, se indican todas las máquinas que usan un perfil de alertas seleccionado.

Tableros

AntiMalware > Mostrar > Tableros

En la página **Tableros**, se proporciona una vista de tablero del estado de las máquinas que tienen instalado **AntiMalware**. Las estadísticas del tablero que se muestran dependen del **filtro ID de máquina/ID de grupo** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)* y de los grupos de máquinas que el usuario está autorizado a ver en Sistema > **Ámbitos** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4578.htm)*.

Acciones

- **Acciones**
  - **Nuevo**: crea un tablero nuevo.
  - **Guardar**: guarda los cambios en el tablero que se muestra en ese momento.
  - **Guardar como**: guarda el tablero que se muestra en ese momento con un nombre nuevo.
  - **Eliminar**: elimina el tablero que se muestra en ese momento.
- **Seleccionar tablero**: selecciona un tablero para mostrar.
- **Agregar partes**: agrega partes al tablero que se muestra en ese momento. Consulte la lista de partes a continuación.
- **Abrir en otra ventana**: muestra el tablero seleccionado en una pestaña o una ventana aparte.

Partes del tablero de AntiMalware

- **Extensión automática de licencia de AntiMalware**: gráfico de barras en el que se muestra la cantidad de máquinas que tienen una extensión automática de licencia establecida en 30, 60, 90 o más de 91 días.
- **Recuento de licencias de AntiMalware**: gráfico de barras en el que se muestra la cantidad de licencias de **AntiMalware** utilizadas y la cantidad de máquinas que tienen una instalación pendiente.
- **Vencimiento de licencia de AntiMalware**: gráfico de barras en el que se muestra la cantidad de máquinas cuyas licencias vencieron o vencen en 30, 60, 90 o más de 91 días.
- **Resumen de licencias de AntiMalware**: en un gráfico, se muestra la cantidad de máquinas que están `Available`, `Expired`, `In Use`, `Partials` y `Pending Install`.
- **Máquinas con AntiMalware que necesitan atención**: gráfico de barras en el que se muestra la cantidad de máquinas administradas que cuentan con **AntiMalware** que necesitan atención, según su categoría. Las categorías incluyen `No AM Installed`, `With Uncured Threats`, `Out of Date`, `Reboot Needed`, `Component Status`.
- **Máquinas con AntiMalware con detecciones**: gráfico de barras en el que se muestra el número de detecciones.
- **Estado de protección de AntiMalware**: gráfico circular en el que se muestran categorías de porcentajes de máquinas con protección de **AntiMalware**. Las categorías de porcentajes incluyen `Not Installed`, `Out of Date`, `Not Enabled` y `Up to Date`.
- **Principales amenazas que detecta AntiMalware**: se enumeran las máquinas con la mayor cantidad de amenazas. Al hacer clic en la ID de máquina con hipervínculo, se muestran las amenazas que pertenecen a dicha ID de máquina en la página **Detecciones** *(página 11)*.

Detecciones

AntiMalware > Mostrar > Administrar detecciones

En la página **Detecciones**, se muestran amenazas de virus que **AntiMalware** no resuelve automáticamente. Use la información que se incluye en esta página para investigar en profundidad las amenazas y eliminarlas en forma manual. La lista de máquinas que se muestra depende del **filtro ID**

de máquina/ID de grupo *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#209.htm)* y de los grupos de máquinas que el usuario está autorizado a ver en Sistema > **Ámbitos** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4578.htm)*.

Acciones

- **Detalles**: haga clic para obtener más información sobre una amenaza seleccionada en el sitio web Securelist de Kaspersky.
- **Agregar exclusión**: agrega filas seleccionadas a la lista de exclusiones.
- **Eliminar**: envía una solicitud al extremo para eliminar el archivo en cuarentena.
- **Restaurar**: envía una solicitud al extremo para quitar el archivo de cuarentena. El archivo ya no se considera una amenaza.
- **Ocultar**: no mostrar en esta lista. Ocultar la amenaza no significa que se elimine.
- **Filtrar**: filtra la lista según una de las siguientes categorías:
  - **Borrar filtro**: quita todos los filtros de la lista.
  - **Amenazas activas**: se muestran las amenazas de **AntiMalware** que se detectaron, pero que aún no se desinfectaron, eliminaron o excluyeron.
  - **Archivos en cuarentena**: se muestran los archivos en cuarentena.
  - **Archivos eliminados**: se muestra una lista de los archivos eliminados.
  - **Últimos <N períodos> de amenazas**: filtra la lista por uno o varios de los períodos predefinidos.

Columnas de tabla

- **Nombre de la máquina**: el ID de la máquina.
- **Nombre**: el nombre de la amenaza.
- **Ruta**: la ubicación de la amenaza en la máquina administrada.
- **Hora**: la fecha y la hora en que se detectó la amenaza.
- **Estado**: el estado de la amenaza. Los mensajes de estado incluyen, entre otros, lo siguiente:
  - *Detección por detector*
    - ✓ `Failed to unload process`: es posible que se necesite reiniciar para completar la eliminación de malware.
    - ✓ `Unloaded process successfully`
    - ✓ `Delete on reboot`: es necesario reiniciar para completar la eliminación de malware.
    - ✓ `Quarantined and deleted successfully`
    - ✓ `Not selected for removal`: no se seleccionó el elemento y, probablemente, no sea una amenaza.
  - *Detección por módulo de protección*
    - ✓ `ALLOW`: el usuario hizo clic en **Omitir** durante una detección de malware.
    - ✓ `QUARANTINE`: el usuario hizo clic en **Cuarentena** durante una detección de malware.
    - ✓ `DENY`: el usuario hizo clic en **Cuarentena** durante una detección de malware, pero el bloqueo no fue satisfactorio o la detección ya estaba bloqueada.
- **Tipo**: la categoría de la amenaza.
- **Nombre de perfil**: el nombre del perfil que estaba en uso cuando se detectó la amenaza.

Perfiles

AntiMalware > Configuración > Perfiles

En la página **Perfiles**, se administran los perfiles de **AntiMalware**. Cada perfil representa un conjunto distinto de opciones de **AntiMalware** habilitadas o deshabilitadas. Los cambios en un perfil afectan a

todos los ID de máquina asignados a ese perfil. Los perfiles se asignan a los ID de máquina en AntiMalware > **Máquinas** *(página 3)* > **Asignar**. En general, los diferentes tipos de máquinas o redes requieren diferentes perfiles. Los perfiles sólo son visibles si el usuario creó el perfil o si el perfil se asignó a una máquina asignada al ámbito que se está utilizando.

Tipos de perfil: Sólo estaciones de trabajo

Los perfiles de **AntiMalware** sólo se pueden asignar a estaciones de trabajo. Se proporciona un perfil de ejemplo.

Acciones

- **Nuevo perfil**: crea un nuevo perfil de configuración. Los perfiles admiten las versiones 1.75 de antimalware de Malwarebytes.
- **Abrir**: abre un perfil existente para editarlo. También puede hacer doble clic en un perfil para abrirlo.
- **Eliminar**: elimina un perfil existente.
- **Guardar**: guarda los cambios en el perfil seleccionado en ese momento.
- **Copiar**: guarda el perfil seleccionado con un nombre nuevo.

Adición y edición de perfiles

Haga clic en **Nuevo** y, a continuación, en un *tipo de perfil*, para visualizar la ventana **Nuevo perfil**, o haga clic en un perfil existente y, a continuación, en **Abrir** para visualizar la ventana **Editar perfil**.

- **Pestaña Resumen** *(página 17)*
- **Pestaña Protección** *(página 13)*
- **Pestaña Análisis AM** *(página 14)*
- **Pestaña Opciones de actualización** *(página 15)*
- **Pestaña Exclusiones** *(página 15)*
- **Pestaña Extremos** *(página 16)*

Columnas de tabla

- **Nombre**: nombre del perfil.
- **Tipo de perfil**: `Anti-Malware`
- **Máquinas aplicadas**: cantidad de máquinas que utilizan este perfil.
- **Creado por**: usuario del VSA que creó este perfil.
- **Versión:** `KAM 1.75`

Pestaña Resumen

AntiMalware > Configuración > Perfiles > pestaña Resumen

- **Nombre**: el nombre del perfil.
- **Descripción**: una descripción del perfil.
- **Tipo de perfil**: estación de trabajo de **AntiMalware**.
- **Versión del perfil:** `KAM 1.75`

Pestaña Protección

AntiMalware > Configuración > Perfiles > Protección

- **Iniciar módulo de protección con Windows**: si está seleccionada, el módulo de protección se inicia junto con Windows.

- **Iniciar bloqueo de ejecución de archivo cuando se inicia el módulo de protección**: si está seleccionada, se inicia el bloqueo de ejecución de archivo cuando se inicia el módulo de protección.
- **Iniciar bloqueo de sitios web malintencionados cuando se inicia el módulo de protección**: si está seleccionada, se inicia el bloqueo de sitios web malintencionados cuando se inicia el módulo de protección.
  - **Mostrar globo de información cuando se bloquea un sitio web malintencionado**: si está seleccionada, se muestra un globo de información al usuario cuando se bloquea un sitio web malintencionado.

Pestaña Análisis AM

AntiMalware > Configuración > Perfiles > Análisis AM

En la pestaña **Análisis AM**, se programan análisis periódicos para un perfil de **AntiMalware** seleccionado.

- **(Tipo de programación)**
  - `Manually`: los análisis de las máquinas con este perfil sólo se programan en forma manual.
  - `By Schedule`: permite programar los análisis de las máquinas con este perfil en la cantidad de períodos especificada. El tiempo se basa en el agente.
- **(Tipo de análisis)**
  - `Full`: en este análisis, se analizan todos los archivos en las unidades seleccionadas. En la mayoría de los casos, se recomienda un análisis rápido.
  - `Quick`: en este análisis, se utiliza una tecnología de análisis de sistemas veloz para detectar software malintencionado.
  - `Flash`: en este análisis, se analizan la memoria y los objetos de ejecución automática.
- **(Intervalo de análisis)**
  - `<Period>/Run every/On Reboot` : seleccione los períodos usados para especificar el intervalo entre análisis de **AntiMalware**. En forma alternativa, puede elegir que el análisis se lleve a cabo sólo cuando se reinicia la máquina.
- **Recuperar si no se ejecutó después de (horas)**: la cantidad de horas que se debe esperar para volver a intentar ejecutar el análisis si la máquina no estuvo disponible a la hora programada.
- **Hora de ejecución del análisis**: hora en que el agente debe comenzar un análisis único o periódico.
- **Fecha de ejecución del análisis**: fecha en que el agente debe comenzar un análisis único o periódico.
- **Reiniciar la computadora si es necesario como parte de la eliminación de amenazas**: si está seleccionada, la computadora se reinicia para completar la eliminación de amenazas, si es necesario.
- **Eliminar amenazas automáticamente**: si está seleccionada, las amenazas se eliminan automáticamente.
- **Activación desde suspensión**: si está seleccionada, se intenta activar la computadora desde la suspensión para realizar un análisis programado.
- **Habilitar motor de heurística avanzada**: si está seleccionada, se agrega otra capa de protección para detectar malware nuevo o desconocido.
- **Conceder recursos a otras aplicaciones**: si está seleccionada, cuando aumenta la carga en el sistema de archivos de otras aplicaciones, las tareas de análisis se pausan.

Pestaña Opciones de actualización

AntiMalware > Configuración > Perfiles > Opciones de actualización

En la pestaña **Opciones de actualización** para un perfil de **AntiMalware** seleccionado, se programa la descarga de las actualizaciones de **AntiMalware** en los equipos cliente.

- **Descargar e instalar actualización de programa si está disponible**: si está seleccionada, se descargan e instalan las actualizaciones de programas disponibles.
- **(Tipo de programación)**
  - `By Schedule`: permite programar las actualizaciones de las máquinas con este perfil en la cantidad de períodos especificada. El tiempo se basa en el agente.
  - `Manual`: las actualizaciones de las máquinas con este perfil sólo se programan en forma manual. Actualice las máquinas en forma manual en el panel de control de la página **Máquinas** *(página 3)*.
- **(Intervalo de análisis)**
  - `<Period>/Run every/On Reboot` : seleccione los períodos usados para especificar el intervalo entre actualizaciones de **AntiMalware**. En forma alternativa, puede elegir que la actualización se lleve a cabo sólo cuando se reinicia la máquina.
- **Recuperar si no se ejecutó después de (horas)**: la cantidad de horas que se debe esperar para volver a intentar ejecutar la actualización si la máquina no estuvo disponible a la hora programada.
- **Hora de ejecución de la actualización**: hora en que el agente debe comenzar una actualización única o periódica.
- **Fecha de ejecución de la actualización**: fecha en que el agente debe comenzar una actualización única o periódica.
- **Activar la computadora desde la suspensión para realizar la tarea**: si está seleccionada, se activa la computadora para realizar la actualización, si es necesario.
- **Ejecutar análisis de flash después de una actualización correcta**: si está seleccionada, se ejecuta un análisis de flash después de la actualización.
- **Usar configuración personalizada del servidor proxy**: si está seleccionada, se usa un servidor proxy para descargar actualizaciones.
  - **Dirección**: introduzca una dirección IP o un nombre de servidor proxy válidos.
  - **Puerto** : ingrese un número de puerto.
- **Especificar datos de autenticación**: si está seleccionada, se requiere la autenticación de proxy.
  - **Nombre de usuario**: si está seleccionada la opción **Especificar datos de autenticación**, introduzca un nombre de usuario válido.
  - **Contraseña cifrada**: si está seleccionada la opción **Especificar datos de autenticación**, introduzca una contraseña válida.
- **Omitir el servidor proxy para la dirección local**: si está seleccionada, las máquinas que están en la misma red que el servidor proxy no lo utilizan.

Pestaña Exclusiones

AntiMalware > Configuración > Perfiles > Exclusiones

En la pestaña **Exclusiones** para los perfiles de **AntiMalware**, se excluyen objetos de la supervisión de **AntiMalware**.

Reglas de exclusión

- **Agregar exclusión**: se agregan entradas para excluirlas del análisis y la protección, con un límite de 256 exclusiones. No se admiten comodines.

- **Archivo o carpeta**: las rutas de archivos o carpetas deben comenzar con una letra de unidad. Ejemplos: `C:\Windows\file.exe` O `C:\Windows\folder`
- **Clave o valor de registro**: las claves y los valores de registro deben comenzar con un nombre de subárbol válido, como `HKCU`, `HKLM`, `HKCR`, `HKU`. Ejemplos: `HKLM\Software\key` O `HKLM\Software\key|value`
- **IP**, por ejemplo: `111.222.33.444`

- **Eliminar**: elimina una regla de exclusión seleccionada.

Pestaña Extremos

AntiMalware > Configuración > Alertas > Extremos

En la pestaña **Extremos**, se enumeran todas las máquinas que usan el perfil de alertas seleccionado.

Nota: En la pestaña **Perfiles de alerta** en Máquinas > **Detalles** *(página 9)*, se muestra la lista de **perfiles de alerta** *(página 9)* asignados a una máquina seleccionada.

Alertas

AntiMalware > Configuración > Alertas

En la página **Alertas**, se administran los perfiles de alerta de **AntiMalware**. Cada perfil de alerta representa un conjunto diferente de condiciones de alerta y de acciones que se realizan ante una situación de alerta. Se pueden asignar varios perfiles de alerta al mismo extremo. Los cambios en un perfil de alerta afectan a todos los ID de máquina asignados a ese perfil. Se asigna un perfil de alerta a los ID de máquina en AntiMalware > **Máquinas** *(página 3)* > **Perfiles de alerta**. Los diferentes tipos de máquinas pueden requerir diferentes perfiles de alerta. Los perfiles de alerta están visibles para todos los usuarios del VSA.

Nota: Los perfiles de alerta creados en **Antivirus** o **AntiMalware** pueden verse y editarse en ambos productos. Si se asigna un perfil de alerta a una máquina mediante **Antivirus** o **AntiMalware**, el perfil de alerta se asigna a ambos productos en esa máquina.

Revisión de alarmas creadas por alertas de AntiMalware

- Monitor > **Resumen de alarmas** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#1959.htm)*
- Monitor > Lista de tablero > cualquier **ventana Resumen de alarmas** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4112.htm)* dentro de un dashlet
- Agente > Registros de agente > **Registro de agente** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#354.htm)*
- Agente > Registros de agente > **Registro de acciones de supervisión** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#354.htm)*: muestra las medidas que se toman ante una situación de alerta, se haya creado una alarma o no.
- **Live Connect** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#4796.htm)* > Datos de agente > Registros de agente > Registro de alarmas
- Info Center > Elaboración de informes > Informes heredados > Registros > Registro de alarmas

Acciones

- **Nuevo**: crea un nuevo perfil de alerta.
- **Abrir**: abre un perfil de alerta existente para editarlo. También puede hacer doble clic en un perfil de alerta para abrirlo.

- **Eliminar**: elimina un perfil de alerta existente.
- **Guardar**: guarda los cambios en el perfil de alerta seleccionado en ese momento.
- **Copiar**: guarda el perfil de alerta seleccionado con un nombre nuevo.
- **Configuración de alertas**: configura el formato de cada tipo de mensaje de notificación de alerta.

Adición y edición de perfiles

Haga clic en **Nuevo** para visualizar la ventana **Nuevo perfil de alerta** o haga clic en un perfil existente y, a continuación, en **Abrir** para visualizar la ventana **Editar perfil de alerta**.

- **Pestaña Resumen** *(página 13)*
- **Pestaña Tipos de alerta** *(página 17)*
- **Pestaña Acciones** *(página 18)*
- **Pestaña Extremos** *(página 18)*

Columnas de tabla

- **Nombre**: nombre del perfil de alerta.
- **Descripción**: una descripción del perfil de alerta.

Pestaña Resumen

AntiMalware > Configuración > Alertas > pestaña Resumen

- **Nombre**: el nombre del perfil de alerta.
- **Descripción**: una descripción del perfil de alerta.

Pestaña Tipos de alerta

AntiMalware > Configuración > Alertas > pestaña Tipos de alerta

Nota: Cuando se establece una alerta para KAM 6.5, también se la establece para KAV 6.5.

Selección de alertas y datos de configuración

- **Seguridad eliminada por el usuario**: se desinstaló un producto de seguridad administrada del extremo.
- **Protección deshabilitada (totalidad del motor)**: se deshabilitó la protección de un producto de seguridad administrada.
- **Definición no actualizada en X días/número de días**: las definiciones de un producto de seguridad administrada no se actualizaron en un número de días específico.
- **Actualización de definición incompleta**: no se completó la actualización de las definiciones de un producto de seguridad administrada.
- **Amenaza activa detectada**: se detectó una amenaza activa. Una amenaza activa es una detección que no se subsanó ni se eliminó. Se requiere la intervención del usuario en la página **Detecciones** *(página 11)*.
- **Amenaza detectada y subsanada**: se detectó una amenaza y se la subsanó. No se requiere intervención del usuario.
- **Análisis incompleto**: no se completó el análisis.
- **Reinicio requerido**: se requiere un reinicio.
- **La licencia vence en X días/número de días**: una licencia vence en un número de días específico.

- **La licencia venció y no se renovó**: la licencia de un producto de seguridad administrada venció y no se renovó.
- **Perfil no compatible**: un extremo no es compatible con su perfil.
- **Error en la asignación de perfil**: se produjo un error en la asignación de un perfil a una máquina.
- **Error en la instalación del cliente**: se produjo un error en la instalación de un producto de seguridad administrada.
- **Error en la reparación del cliente**: se produjo un error en la reparación de un producto de seguridad administrada.
- **Error en la desinstalación del cliente**: se produjo un error en la desinstalación de un producto de seguridad administrada.

Pestaña Acciones

AntiMalware > Configuración > Alertas > pestaña Acciones

En la pestaña **Acciones** de un perfil de alerta, se determinan las acciones que se llevan a cabo ante cualquiera de los **Tipos de alerta** *(página 17)* que encuentra un extremo asignado a ese perfil de alerta.

- **Crear alarma**: si está seleccionada y se encuentra un tipo de alerta, se crea una alarma.
- **Crear ticket**: si está seleccionada y se encuentra una condición de alerta, se crea un ticket.
- **Destinatarios de correo electrónico (separados por coma)**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
- **Ejecutar script**: si está seleccionada y se encuentra una condición de alerta, se ejecuta un procedimiento de agente.
  - **Nombre de script**: seleccione el nombre del procedimiento de agente.
- **Enviar mensaje a Info Center**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
  - **Seleccionar usuarios para notificar**: seleccione los usuarios a los que se les debe notificar alertas de **AntiMalware** en Info Center > **Buzón de entrada** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#9460.htm)*.
- **Enviar mensaje a barra de notificación**: si está seleccionada y se encuentra una condición de alerta, se envía un correo electrónico a las direcciones especificadas.
  - **Seleccionar usuarios para notificar**: seleccione los usuarios a los que se les debe notificar de las alertas de **AntiMalware** en la **barra de notificación** *(http://help.kaseya.com/webhelp/ES/VSA/7000000/index.asp#10634.htm)*.

Pestaña Extremos

AntiMalware > Configuración > Perfiles > Extremos

En la pestaña **Extremos**, se enumeran todas las máquinas que usan el perfil de **AntiMalware** seleccionado.

Índice

A

Alertas • 16

C

Columnas de AntiMalware • 8
Cuadrícula de explorador • 4

D

Detecciones • 11
Diseño de página • 3

I

Introducción a AntiMalware • 1

M

Máquinas • 3

P

Panel de control • 5
Panel de detalles • 9
Perfiles • 12
Pestaña Acciones • 18
Pestaña Análisis AM • 14
Pestaña Exclusiones • 15
Pestaña Extremos • 16, 18
Pestaña Opciones de actualización • 15
Pestaña Protección • 13
Pestaña Resumen • 13, 17
Pestaña Tipos de alerta • 17

R

Requisitos del módulo AntiMalware • 3

T

Tableros • 11